

Notice of Allowability	Application No.	Applicant(s)
	09/912,391	HURSEY ET AL.
	Examiner	Art Unit
	MATTHEW T. HENNING	2431

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTO-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. This communication is responsive to the request for continued examination filed 11/23/2009.
2. The allowed claim(s) is/are 1-4,6-12,14-20 and 22-28.
3. Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All
 - b) Some*
 - c) None
 of the:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) hereto or 2) to Paper No./Mail Date _____.
 - (b) including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. Notice of References Cited (PTO-892)
2. Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____
4. Examiner's Comment Regarding Requirement for Deposit
of Biological Material
5. Notice of Informal Patent Application
6. Interview Summary (PTO-413),
Paper No./Mail Date 12/10/2009.
7. Examiner's Amendment/Comment
8. Examiner's Statement of Reasons for Allowance
9. Other _____.

/Matthew T Henning/
Primary Examiner, Art Unit 2431

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Jamie Rossi on December 10, 2009.

The examiner notes that no new matter has been entered by this amendment.

The application has been amended as follows:

Please replace the paragraph beginning on line 21 of page 9 of the specification with the following paragraph:

It will be appreciated that the general purpose computer 200 operating under control of a suitable computer program may perform the above described techniques and provide apparatus for performing the various tasks described. The general purpose computer 200 also executes the method described previously. The computer program product could take the form of a ~~recordable computer readable storage~~ medium bearing the computer program, such as a floppy disk, a compact disk or other ~~recordable computer readable storage~~ medium. Alternatively, the computer program could be dynamically downloaded via the network interface unit 220.

Please amend claim 1 as follows:

1. (Currently Amended) A computer program product comprising a computer readable storage medium bearing a computer program operable to control an e-mail client computer to detect e-mail propagated malware, said computer program product comprising:
e-mail generating logic operable to generate an e-mail message;
comparison logic operable to compare said e-mail message with at least one of an address book of a sender of said e-mail message and one or more previously generated e-mail messages from said client computer; and
identifying logic operable to identify whether:
(i) said e-mail message is being sent to more than a threshold number of addressees specified within said address book;
(ii) said e-mail message contains message content having at least a threshold level of similarity to non-identical message content of said previously generated e-mail messages being sent to more than a threshold number of addressees specified within said address book; and
(iii) said e-mail message contains message content having at least a threshold level of similarity to non-identical message content of more than a threshold number of said previously generated e-mail messages;
wherein said identifying logic is further operable to identify said email message as potentially containing malware if at least one of items (i), (ii), and (iii) is identified; and

quarantine queue logic operable to hold said previously generated e-mail messages in a quarantine queue for at least a predetermined quarantine period prior to being sent from said client computer;

wherein said quarantine queue logic is further operable such that it is determined whether said email message is a new message by comparing said email message with said previously generated e-mail messages held in said quarantine queue;

wherein said quarantine queue logic is further operable such that said email message is added to said quarantine queue in response to a determination that said email message is said new message;

wherein said quarantine queue logic is further operable such that a score value indicative of one of said previously generated e-mail messages held in said quarantine queue is updated in response to a determination that said email message is not said new message, said score value indicating a proportion of said addressees specified within said address book that have previously been sent said message sharing at least said threshold level of similarity to non-identical message content of said one of said previously generated e-mail messages.

Please amend claim 17 as follows:

17. (Currently Amended) Apparatus for detecting e-mail propagated malware within a client computer, said apparatus comprising:

an e-mail generator operable to generate an e-mail message;

a ~~comparator~~ comparator operable to compare said e-mail message with at least one of an address book of a sender of said e-mail message and one or more previously generated e-mail messages from said client computer;

a malware identifier operable to identify whether:

(i) said e-mail message is being sent to more than a threshold number of addressees specified within said address book;

(ii) said e-mail message contains message content having at least a threshold level of similarity to non-identical message content of said previously generated e-mail messages being sent to more than a threshold number of addressees specified within said address book; and

(iii) said e-mail message contains message content having at least a threshold level of similarity to non-identical message content of more than a threshold number of said previously generated e-mail messages;

wherein said malware identifier is further operable to identify said email message as potentially containing malware if at least one of items (i), (ii), and (iii) is identified; and a quarantine queue operable to hold said previously generated e-mail messages in a quarantine queue for at least a predetermined quarantine period prior to being sent from said client computer;

wherein said quarantine queue is further operable such that it is determined whether said email message is a new message by comparing said email message with said previously generated e-mail messages held in said quarantine queue;

wherein said quarantine queue is further operable such that said email message is added to said quarantine queue in response to a determination that said email message is said new message;

wherein said quarantine queue is further operable such that a score value indicative of one of said previously generated e-mail messages held in said quarantine queue is updated in response to a determination that said email message is not said new message, said score value indicating a proportion of said addressees specified within said address book that have previously been sent said message sharing at least said threshold level of similarity to non-identical message content of said one of said previously generated e-mail messages.

Allowable Subject Matter

The following is an examiner's statement of reasons for allowance:

Applicant's arguments, see the remarks, filed 11/23/2009, with respect to claims 1, 9, and 17 have been fully considered and are persuasive. The rejection of the claims has been withdrawn.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MATTHEW T. HENNING whose telephone number is (571)272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571)272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Matthew T Henning/
Primary Examiner, Art Unit 2431